ADVANCES IN MATHEMATICS 29, 11–14 (1978)

Un contre-exemple pour les formes invariantes sur un corps fini

J. DÉSARMÉNIEN

Département de Mathématique, Université de Strasbourg,
7, rue René Descartes, 67084 Strasbourg Cédex, France

Le premier théorème fondamental de la théorie des invariants fournit une caractérisation des formes invariantes, à coefficients dans un corps K, en termes de combinaisons linéaires de produits d'un même nombre de déterminants d'ordre maximal. Ce résultat est connu depuis longtemps lorsque la caractéristique du corps K est zéro. Doubilet, Rota et Stein [1] l'ont étendu au cas des corps quelconques, mais infinis. Suivant une suggestion de Rota, nous nous proposons, dans cette note, en construisant un contre-exemple explicite, de montrer que ce théorème fondamental est en défaut lorsque K est fini. On utilise les notations introduites dans [2] et rappelées ci-dessous pour la commodité du lecteur.

Etant donné un corps K et deux alphabets $\mathscr{X} = \{x_1, x_2, \ldots, x_n\}$ et $\mathscr{U} = \{u_1, u_2, \ldots, u_d\}$, considérons l'algèbre P des polynômes sur K à nd indéterminées, notées $(x_i \mid u_j)$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant d$. Les éléments de P sont appelés *formes*. Une transformation linéaire inversible L, donnée par une matrice (l_{jk}) carrée inversible de dimension $d \times d$, agit sur P de la façon suivante:

$$L(x_i \mid u_j) = \sum_{1 \leqslant k \leqslant d} l_{kj}(x_i \mid u_k), \qquad 1 \leqslant i \leqslant n, \quad 1 \leqslant j \leqslant d.$$

Une forme F est *invariante* lorsque, pour toute transformation linéaire inversible L, il existe une constante $a(L)$ telle que $LF = a(L)F$. Etant données d lettres $x_{i_1}, x_{i_2}, \ldots, x_{i_d}$ de $\mathscr{X}$, le déterminant

$$\begin{vmatrix} (x_{i_1} \mid u_1) & \cdots & (x_{i_1} \mid u_d) \\ \vdots & & \vdots \\ (x_{i_d} \mid u_1) & \cdots & (x_{i_d} \mid u_d) \end{vmatrix},$$

noté $(x_{i_1} \cdots x_{i_d} \mid u_1 \cdots u_d)$ est une forme invariante: la constante $a(L)$ est ici le déterminant de L.

Le premier théorème fondamental de la théorie des invariants s'énonce commodément en termes de bitableaux et de bidéterminants. Etant donnés un entier et un partage (λ) de cet entier, un *bitableau* est une paire $[T, T']$ de tableaux

0001-8408/78/0291–0011$05.00/0

de Young de même forme (λ); le tableau T est rempli avec des lettres de $\mathscr{X}$ et le tableau T' avec des lettres de $\mathscr{U}$. Par exemple,

$$\begin{bmatrix} x_1 & u_3 \\ x_2x_3 & , \ u_1u_2 \\ x_1x_2x_3 & u_1u_3u_4 \end{bmatrix}$$

est un bitableau de forme (3, 2, 1). Le bitableau $[T, T']$ est *standard* lorsque, dans T et dans T' les indices des variables vérifient les deux conditions:

— croissance stricte de gauche à droite dans chaque ligne,
— croissance au sens large dans chaque colonne.

Le bitableau de l'exemple précédent n'est pas standard, par contre, le bitableau

$$\begin{bmatrix} x_2 & u_3 \\ x_1x_3 & , \ u_1u_3 \\ x_1x_2x_3 & u_1u_2u_4 \end{bmatrix}$$

est standard.

Etant données deux suites finies $(x_{i_1}, x_{i_2}, \ldots, x_{i_p})$ et $(u_{j_1}, u_{j_2}, \ldots, u_{j_p})$ de variables de $\mathscr{X}$ et $\mathscr{U}$ respectivement, leur *produit induit* est l'élément de l'algèbre P défini par le déterminant

$$\begin{vmatrix} (x_{i_1} \mid u_{j_1}) & (x_{i_1} \mid u_{j_2}) & \cdots & (x_{i_1} \mid u_{j_p}) \\ (x_{i_2} \mid u_{j_1}) & (x_{i_2} \mid u_{j_2}) & \cdots & (x_{i_2} \mid u_{j_p}) \\ \vdots & \vdots & & \vdots \\ (x_{i_p} \mid u_{j_1}) & (x_{i_p} \mid u_{j_2}) & \cdots & (x_{i_p} \mid u_{j_p}) \end{vmatrix}$$

et noté $(x_{i_1}x_{i_2}\cdots x_{i_p} \mid u_{j_1}u_{j_2}\cdots u_{j_p})$. Le *bidéterminant* du bitableau $[T, T']$ est l'élément de P obtenu en faisant le produit des produits induits de chaque ligne de T par la ligne correspondante de T'; il est noté $(T \mid T')$. Par exemple,

$$\begin{pmatrix} x_2 & u_3 \\ x_1x_3 & u_1u_3 \\ x_1x_2x_3 & u_1u_2u_4 \end{pmatrix} = (x_1x_2x_3 \mid u_1u_2u_4)(x_1x_3 \mid u_1u_3)(x_2 \mid u_3)$$

est somme de $3! \times 2! \times 1! = 12$ monômes de P.

Le premier théorème fondamental de la théorie des invariants repose sur le théorème de la base [2, théorème 2.1. p. 19] dont nous rappelons l'énoncé.

THÉORÈME. *Le bidéterminant d'un bitableau de forme* (λ) *est combinaison*

linéaire à coefficients entiers de bidéterminants de bitableaux standards de même forme, ou de forme lexicographiquement plus longue.

THÉORÈME (Premier théorème fondamental de la théorie des invariants). *Toute forme invariante de P est combinaison linéaire de bidéterminants standards rectangulaires ayant même nombre de lignes; chacune de ces lignes est de longueur d.*

Ce théorème est vrai lorsque le corps de base K est infini, quelle que soit sa caractéristique (cf. [1, 2, p. 31]). Il est faux lorsque K est fini, comme le montre le contre-exemple ci-après.

Prenons $K = \mathbb{F}_2$, corps à deux éléments, et $d = 2$. Les transformations qui agissent sur P sont ici les éléments de $\mathrm{GL}_2(\mathbb{F}_2)$. Ce groupe est engendré par les deux transformations de matrices $L_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ et $L_2 = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Une forme de P est donc invariante si, et seulement si elle est invariante par L_1 et L_2. Ces deux transformations agissent ainsi:

$$\begin{aligned} -L_1(x_i \mid u_1) &= (x_i \mid u_2), \\ L_1(x_i \mid u_2) &= (x_i \mid u_1); \\ -L_2(x_i \mid u_1) &= (x_i \mid u_1) + (x_i \mid u_2), \\ L_2(x_i \mid u_2) &= (x_i \mid u_2), \end{aligned}$$

quel que soit i.

Soit

$$F = \begin{pmatrix} x_1 & u_1 \\ x_1 & u_1 \end{pmatrix} + \begin{pmatrix} x_1 & u_2 \\ x_1 & u_1 \end{pmatrix} + \begin{pmatrix} x_1 & u_2 \\ x_1 & u_2 \end{pmatrix};$$

la forme F est donnée par sa décomposition en bidéterminants standards. D'après le théorème de la base, elle *n'est pas* combinaison linéaire de bidéterminants standards dont chaque ligne est de longueur 2. Cependant, cette forme est *invariante*.

En développant F, on obtient:

$$F = (x_1 \mid u_1)^2 + (x_1 \mid u_1)(x_1 \mid u_2) + (x_1 \mid u_2)^2.$$

Puisque F est symétrique en u_1 et u_2, il est clair que $L_1F = F$. Le calcul de L_2F donne:

$$L_2F = ((x_1 \mid u_1) + (x_1 \mid u_2))^2 + ((x_1 \mid u_1) + (x_1 \mid u_2))(x_1 \mid u_2) + (x_1 \mid u_2)^2,$$

soit encore, puisque sur $\mathbb{F}_2$ on a l'identité $(a + b)^2 = a^2 + b^2$,

$$L_2F = (x_1 \mid u_1)^2 + (x_1 \mid u_2)^2 + (x_1 \mid u_1)(x_1 \mid u_2) + (x_1 \mid u_2)^2 + (x_1 \mid u_2)^2,$$

soit, après simplification,

$$L_2F = F.$$

BIBLIOGRAPHIE

1. P. DOUBILET, G.-C. ROTA, AND J. STEIN, On the foundations of combinatorial theory. IX. Combinatorial methods in invariant theory, *Studies in Appl. Math.* **53** (1974), 185–216.
2. G.-C. ROTA, "Théorie combinatoire des invariants classiques" (avec un appendice de J. Désarménien), Séries de Mathématiques Pures et Appliquées, IRMA Strasbourg, Université Louis Pasteur, Strasbourg, 1977.